UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

CONLAN ABU and
RYAN MOORE,

Plaintiffs,

v.

Civil Case No. 20-10747
Honorable Linda V. Parker

STANLEY B. DICKSON and
DICKSON & ASSOCIATES, PC,

Defendants.
_____/

OPINION AND ORDER GRANTING IN PART AND DENYING IN PART DEFENDANTS' MOTION TO DISMISS OR FOR SUMMARY JUDGMENT

This lawsuit arose from a business deal that went sour. Plaintiff Conlan Abu entered into an agreement to purchase certain restaurant assets from The Epicurean Group. Plaintiff Ryan Moore ("Mr. Moore") is a 50% owner of Conlan Abu (collectively "Plaintiffs"). Defendant Stanley Dickson ("Mr. Dickson") was the owner of The Epicurean Group, and he is majority owner of Defendant Dickson & Associates, PC.

During the state court litigation concerning that business dispute, Plaintiffs discovered that Mr. Dickson and Dickson & Associates (collectively "Defendants") had accessed certain emails in Mr. Moore's rmoore@theepicureangroup.com account. In response, Plaintiffs filed the current

lawsuit alleging that such access violated federal law. Specifically, in their Complaint, Plaintiffs assert violations of (I) the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (II) the Federal Wiretap Act, 18 U.S.C. § 2510; (III) the Stored Communications Act, 18 U.S.C. § 2701; and (IV) civil conspiracy.

Defendants have filed a Motion to Dismiss or for Summary Judgment, in which they argue that the Court should abstain and dismiss this action pursuant to the *Colorado River* doctrine or dismiss the action because Plaintiffs' claims fail. (ECF No. 9.) The motion has been fully briefed. (ECF Nos. 10, 11.) At the Court's request, the parties filed supplemental briefs providing updated information concerning the state court litigation between the parties. (ECF Nos. 12, 13.) The Court is dispensing with oral argument with respect to Defendants' motion. *See* E.D. Mich. LR 7.1(f).

I. Relevant Facts & Procedural Background

The Epicurean Group is comprised of several catering operations and restaurants. (Compl. ¶ 8, ECF No. 1 at Pg ID 3.) On January 1, 2019, Conlan Abu entered into an Asset Purchase Agreement to buy most of The Epicurean Group's assets. (Mot. Ex. A, ECF No. 9-2 at Pg ID 104-131.) Prior to and following the sale, Dickson & Associates, through its internet technology ("IT") company, Propel Technologies, paid for and acted as the IT administrator for The Epicurean Group email accounts, which contained the "@theepicureangroup.com" domain

name. (Massey Decl. ¶¶ 3-4, ECF No. 9-4 at Pg ID 193.) All email accounts with this domain name are hosted under Defendants' tenant account. (*Id.* ¶ 4.)

After January 1, 2019, Mr. Moore began using the email address rmoore@theepicureangroup.com. Mr. Moore accessed this email account on his laptop. (Moore Decl. ¶¶ 2, 4, ECF No. 10-5 at Pg ID 453-54.) Mr. Moore had purchased Microsoft Outlook licenses in September 2018, one of which he installed on his laptop. (*Id.*) He added a mailbox in Outlook for his rmoore@theepicureangroup.com email. (*Id.* ¶ 4.)

Defendants, however, continued to pay the license fees associated with the @theepicureangroup.com accounts after the APA's effective date. (Massey Decl. ¶¶ 4, 5, ECF No. 9-4 at Pg ID 193.) Plaintiffs did not ask Defendants to migrate the accounts or data to Plaintiffs. (*Id.* ¶ 8, Pg ID 194.) When Plaintiffs or their employees had issues with their @theepicureangroup.com email accounts, they contacted the IT administrator for the entities associated with Mr. Dickson and Dickson & Associates. (*Id.* ¶¶ 6-7, Pg ID 193.) This individual initially was Chris Godsell, but John Massey subsequently replaced Mr. Godsell. (*Id.*; Moore Decl. ¶¶ 3, 5, ECF No. 10-5 at Pg ID 454-55). Nevertheless, Mr. Moore states that he never expressly designated Mr. Godsell or Mr. Massey to serve as the "administrator" of his email account, nor did Mr. Moore expressly authorize them to access his email. (Moore Decl. ¶¶ 6-7, ECF No. 10-5 at Pg ID 455.) According to Mr. Moore,

Dickson & Associates "was only authorized to help with the 'termination of employees, new hires, creation of new accounts, and resetting passwords.'" (Resp. at 5, ECF No. 10 at Pg ID 371 (quoting Massey Decl. ¶ 7, ECF No. 9-4 at Pg ID 193).)

A dispute arose between the parties to the Asset Purchase Agreement, resulting in Conlan Abu, Mr. Moore, and Mr. Moore's father suing The Epicurean Group, the related businesses, and Mr. Dickson in the Circuit Court for Oakland County, Michigan ("State Court Action").[1] (Mot. Ex. A, ECF No. 9-2.) While the State Court Action was pending, Mr. Massey, at Mr. Dickson's direction, accessed emails to and from Mr. Moore's @theepicureangroup.com address. (Massey Decl. ¶¶ 9, 14, 15, ECF No. 9-4 at Pg ID 194-95.) According to Mr. Massey, while reviewing Mr. Moore's emails, he discovered that certain emails had been deleted. (*Id.* ¶ 14, Pg ID 195.) In fact, he observed emails being deleted while he was viewing the account. (*Id.* ¶ 15.)

The alleged destruction of these emails became the subject of a discovery dispute in the State Court Action. (Mot. Exs. D-H, ECF Nos. 9-5 to 9-9.) While litigating the dispute, discovery was obtained regarding Plaintiffs' email systems, servers, and network storage devices (ECF No. 12 at Pg ID 613-14.) Mr. Massey

[1] The Epicurean Group and the related businesses filed a counter-complaint against Conlan Abu, Mr. Moore, Mr. Moore's father, and several business entities in the State Court Action, in which they allege state law claims related to the APA.

was deposed. (Massey Dep., ECF No. 9-8.) During that deposition, Mr. Massey testified that he had accessed Mr. Moore's @theepicureangroup.com email account, and he explained how he accessed and downloaded data from the epicureangroup.com email server. (Massey Dep. at 54-55, ECF No. 9-8 at Pg ID 233-34.)

As of February 24, 2021, discovery had closed in the State Court Action and dispositive motions were pending. (ECF No. 13 at Pg ID 615.) The parties' supplemental filings do not suggest that any discovery disputes remain unresolved in the State Court Action.

Claiming that Mr. Massey, who was acting at the direction of Defendants, lacked the authority to access Mr. Moore's @theepicureangroup.com email, Plaintiffs filed this federal court action. Plaintiffs assert that the email account was owned and controlled by Mr. Moore, not Defendants. Plaintiffs maintain that Mr. Moore created the account using one of the Microsoft Outlook licenses he obtained when he purchased a Microsoft Office 365 package.

II. *Colorado River* Doctrine

Defendants first urge the Court to dismiss this action pursuant to the doctrine set forth in *Colorado River Water Conservation District v. United States*, 424 U.S. 800 (1976). In that case, the Supreme Court provided that, "despite the 'virtually unflagging obligation of the federal courts to exercise the jurisdiction given them,'

424 U.S. at 817 …. considerations of judicial economy and federal-state comity may justify abstention in situations involving the contemporaneous exercise of jurisdiction by federal and state courts." *Romine v. Compuserve Corp.*, 160 F.3d 337, 339 (6th Cir. 1998). The principles underlying the *Colorado River* doctrine "'rest on considerations of wise judicial administration, giving regard to conservation of judicial resources and comprehensive disposition of litigation.'" *Id*. (quoting *Colorado River*, 424 U.S. at 817) (internal quotation marks, citations, and brackets omitted). *Colorado River* abstention "is only appropriate in extraordinary circumstances." *Baskin v. Bath Twp. Bd of Zoning Appeals*, 15 F.3d 569, 571 (6th Cir. 1994) (citing *Colorado River*, 424 U.S. at 817).

The Sixth Circuit has identified two prerequisites for abstention under the *Colorado River* doctrine. *Romine*, 160 F.3d at 339-40. First, the court must find that there are parallel and concurrent state and federal actions. *Id.* at 339. Second, the court must consider several factors:

> (1) whether the state court has assumed jurisdiction over any res or property; (2) whether the federal forum is less convenient to the parties; (3) avoidance of piecemeal litigation; (4) the order in which jurisdiction was obtained … (5) whether the source of governing law is state or federal; (6) the adequacy of the state court action to protect the federal plaintiff's rights; (7) the relative progress of the state proceedings; and (8) the presence or absence of concurrent jurisdiction.

Id. at 340-41 (internal citations omitted).

As to the first requirement, "[e]xact parallelism is not required; it is enough if the two proceedings are substantially similar." *Id*. at 340 (original brackets, quotation marks, and citations omitted). Because the parties were substantially similar and the claims were predicated on the same allegations as to the same material facts, the *Romine* court found the actions to be parallel even though the federal action included parties not present in the state proceedings. *Id*.; *see also Heitmanis v. Austin*, 899 F.2d 521, 528 (6th Cir. 1990). When deciding whether the actions are parallel, a "district court must compare the issues in the federal action to the issues actually raised in the state court action, not those that might have been raised." *Baskin*, 15 F.3d at 572. Lawsuits "'predicated on the same allegations as to the same material facts,'" may be parallel even if they do not involve identical causes of action. *Healthcare Co. Ltd. v. Upward Mobility, Inc.*, 784 F. App'x 390, 394 (6th Cir. 2019) (citing *Romine*, 160 F.3d at 340).

Here, the federal and state actions are not parallel. There is "substantial symmetry" between the parties to the two actions. *Preferred Care of Delaware, Inc. v. VanArsdale*, 676 F. App'x 388, 394 (6th Cir. 2017). However, the two lawsuits are not predicated on the same allegations as to the same material facts. The State Court Action arises from the sale of the Epicurean Group. This federal litigation arises from conduct that arose during discovery in the State Court Action. Even if the state court was previously asked to address that conduct—specifically

when deciding whether one of the parties violated the state's discovery rules—the State Court Action in no way involved or resolved the violations of federal law asserted in the present matter.

Because the state and federal actions are not parallel, the Court finds it unnecessary to analyze the factors relevant to deciding whether *Colorado River* abstention is appropriate. The Court concludes that *Colorado River* abstention is not appropriate.

III. The Viability of Plaintiffs' Claims

Defendants alternatively argue that Plaintiffs' claims fail on the merits and therefore should be dismissed pursuant to Federal Rule of Civil Procedure 12(b)(6) or, alternatively, are not supported by the evidence and therefore Defendants are entitled to summary judgment under Rule 56.

As an initial matter, Plaintiffs argue in their response brief that Defendants' motion for summary judgment is premature because the parties have not begun discovery in this case. (Resp. at 24-25, ECF No. 10 at Pg ID 390-91.) In a declaration attached to Plaintiffs' response, Mr. Moore identifies several facts he purportedly cannot present to support his opposition due to the lack of discovery. (Moore Decl. ¶ 9, ECF No. 10-5 at Pg ID 456-47.) The Court will address Plaintiffs' purported need for additional discovery where relevant, as not all of

Plaintiffs' claims or Defendants' arguments for dismissal hinge on those unknown facts.

A. Applicable Standards

A motion to dismiss pursuant to Rule 12(b)(6) tests the legal sufficiency of the complaint. *RMI Titanium Co. v. Westinghouse Elec. Corp.*, 78 F.3d 1125, 1134 (6th Cir. 1996). "To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). In deciding whether the plaintiff has set forth a "plausible" claim, the court must accept the factual allegations in the complaint as true. *Erickson v. Pardus*, 551 U.S. 89, 94 (2007). This presumption is not applicable to legal conclusions, however. *Iqbal*, 556 U.S. at 668. Therefore, "[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Id*. (citing Twombly, 550 U.S. at 555).

Summary judgment pursuant to Federal Rule of Civil Procedure 56 is appropriate "if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). The central inquiry is "whether the evidence presents a sufficient disagreement to require submission to a jury or whether it is so one-sided that one

party must prevail as a matter of law." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 251-52 (1986).

The movant has the initial burden of showing "the absence of a genuine issue of material fact." *Id*. at 323. Once the movant meets this burden, the "nonmoving party must come forward with specific facts showing that there is a genuine issue for trial." *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 587 (1986) (internal quotation marks and citation omitted). To demonstrate a genuine issue, the nonmoving party must present sufficient evidence upon which a jury could reasonably find for that party; a "scintilla of evidence" is insufficient. *See Liberty Lobby*, 477 U.S. at 252. The court must accept as true the non-movant's evidence and draw "all justifiable inferences" in the non-movant's favor. *See Liberty Lobby*, 477 U.S. at 255.

B. Computer Fraud & Abuse Act

In Count I of their Complaint, Plaintiffs allege that Mr. Massey's unauthorized access of Mr. Moore's @theepicureangroup emails violated the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030.

Congress first enacted the CFAA to deter computer crime. *Estes Forwarding Worldwide LLC v. Cuellar*, 239 F. Supp. 3d 918, 922 (E.D. Va. 2017). "While the CFAA is primarily a criminal statute designed to combat hacking, *see A.V. ex rel Vanderhye v. iParadigms, LLC*, 562 F.3d 630, 645 (4th Cir. 2009), it

grants "[a]ny person who suffers damage or loss by reason of a violation of [§ 1030]" the power to bring a civil action "to obtain compensatory damages and injunctive relief or other equitable relief[,]" provided "the conduct involves 1 of the factors set forth in § 1030(c)(4)(A)(i)(1)-(4)]." 18 U.S.C. § 1030(g). The statute provides, in relevant part, that one who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains ... information from any protected computer" and one who "intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss" can be subject to a fine or imprisonment. 18 U.S.C. § 1030(a)(2)(C), (5)(C).

To successfully state a claim under the CFAA, the plaintiff must allege that the defendant:

> (1) intentionally (2) accessed a computer (3) without authorization or in such a way that exceeded his authorized access, and (4) obtained information (5) from any "protected computer," (6) resulting in a loss to one or more persons during any one-year period aggregating at least $5,000 in value.

Estes Forwarding Worldwide, 239 F. Supp. 3d at 922-23; *see also Am. Furukawa, Inc. v. Hossain*, 103 F. Supp. 3d 864, 870 (E.D. Mich. 2015). Defendants argue that Plaintiffs fail to plausibly allege facts to satisfy the fifth and sixth elements and that the record reflects that any access was authorized and within the scope of the authorized access.

i. Protected Computer

Defendants argue that their conduct did not violate the CFAA because Mr. Massey did not access a "computer," but rather a cloud-based email account via the internet.

The CFAA defines "computer" as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."[2] 18 U.S.C. § 1030(e)(1). Defendants cite three cases in support of their argument that this definition does not encompass a cloud-based email account: *Owen v. Cigna*, 188 F. Supp. 3d 790, 793 (N.D. Ill. 2016); *Christie v. Nat'l Inst. for Newman Studies*, No. 16-6573, 2019 WL 1916204, *6 (D.N.J. April 30, 2019); *Brooks v. Agate Res., Inc.*, No. 6:15-cv-00983, 2019 WL 2635594, at *24 (D. Or. Mar. 25, 2019). The courts in *Christie* and *Brooks* relied primarily on *Owen*.

In *Owen,* an employee used her work computer to access personal emails that were stored on an internet-based server. After her employment was terminated, the employer used the computer to access the now-former employee's private email account. The employee sued, alleging that this violated the CFAA.

[2] A "computer" becomes a "protected computer" when it "is used in or affecting interstate or foreign commerce or communication." *Id*. § 1030(e)(2)(B).

Owen, 188 F. Supp. 3d at 791. The District Court for the Northern District of Illinois dismissed the employee's claim, concluding that she lacked the authority to grant or deny anyone permission to access her work computer after she was no longer employed and that "the CFAA is aimed at unauthorized access to computers, not unauthorized access to web-based accounts." *Owen*, 188 F. Supp. 3d at 793.

As Plaintiffs point out, however, "most courts" considering the issue have held that "unauthorized access to web-based accounts can form the basis of a CFAA violation[.]" *Hill v. Lynn*, No. 17 C 06318, 2018 WL 2933636, at *3 (N.D. Ill. June 12, 2018) (citing cases and finding that the plaintiff adequately pled that the defendant accessed a computer within the meaning of the CFAA based on the defendant's access to the plaintiff's web-based account); *Estes Forwarding Worldwide*, 239 F. Supp. 3d at 926-27 (concluding that the plaintiff sufficiently pled access to a "protected computer" by alleging that the defendant accessed its Google drive account from the defendant's personal computer); *RN Entm't, LLC v. Clement*, 380 F. Supp. 3d 711, 719 (M.D. Tenn. 2019) (finding that the plaintiff properly alleged a violation of the statute based on the defendants' withholding passwords, deleting emails, and otherwise impairing the plaintiff's access to its website and email servers after the defendants were terminated); *Brown Jordan Int'l, Inc. v. Carmicle*, No. 0:14-cv-60629, 2016 WL 815827, at *3, *40-41 (S.D.

Fla. Mar. 2, 2015) (concluding that the defendant violated the CFAA when he accessed fellow employees' email accounts through a web portal from his personal ipad); *Hedgeye Risk Mgmt., LLC v. Heldman*, No. 16-935, 2017 WL 4250506, at *7 (D.D.C. Sept. 23, 2017) (the plaintiff pled access to a "protected computer" by alleging that the defendant accessed electronically stored emails and documents via a computer connected to the internet); *see also Russi v. Wissenback*, No. 6:18-cv-01028, 2019 WL 1965830, at *5 (D. Or. Apr. 28, 2019) ("the definition of the terms 'computer' and 'protected' computer' are broad enough to encompass email and financial accounts"). Those courts rely on the inclusion of "data storage facility or communications facility" in the statute's definition of "computer." *Hill*, 2018 WL 2033636, at *3. The Court finds this to be the better interpretation and therefore concludes that Plaintiffs adequately allege that Defendants used a "protected computer" within the meaning of the CFAA.

ii. Damages

As set forth above, to adequately plead a violation of the CFAA, the plaintiff must demonstrate " 'loss' of at least $5,000 in value to one or more persons during any one-year period." *Yoder & Frey Auctioneers, Inc. v. EquipmentFacts, LLC*, 774 F.3d 1065, 1072 (6th Cir. 2014) (citing 18 U.S.C. § 1030(c)(4)(A)(i)(l), (g)). Plaintiffs allege that they incurred "costs in excess of $5,000.00 … to investigate how Defendants obtained unauthorized access to Plaintiff's E-Mails and Email

Account and the extent of the unauthorized access…" (Compl. ¶ 35, ECF No. 1 at Pg ID 8.) Defendants argue that costs associated with an investigation do not qualify as a "loss" under the statute unless the investigation is a direct result of damage to a computer system or interrupted computer service. (Mot. at 15, ECF No. 9 at Pg ID 51 (citing *Am. Family Mut. Ins. Co. v. Rickman*, 554 F. Supp. 2d 766, 772 (N.D. Ohio 2008); *Instant Tech., LLC v. DeFazio*, 40 F. Supp. 3d 989, 1019 (N.D. Ill. 2014), *aff'd* 793 F.3d 748 (7th Cir. 2015).)

The CFAA defines "loss" as:

> any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service[.]

18 U.S.C. § 1030(e)(11). The courts in *American Family* and *Instant Tech* held that the loss must arise from some damage to a computer or the information contained therein. *American Family*, 554 F. Supp. 2d at 772 (internal quotation marks and citations omitted) ("The meaning of 'Loss' both before and after the term was defined by statute, has consistently meant a cost of investigating or remedying damage to a computer or a cost incurred because the computer's service was interrupted."); *Instant Tech*., 40 F. Supp. 3d at 1019 (quotation marks, citation, and brackets omitted) ("'[C]osts not related to computer impairment or computer

damages are not compensable under the CFAA."). The Sixth Circuit, however, reads the statute's definition of loss in the disjunctive:

> ["Loss"] includes "any reasonable cost to any victim including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense." 18 U.S.C. 1030(e)(11). It also encompasses "any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." *Id*. If a plaintiff is able to establish a loss of at least $5,000 in value, whether that be composed solely of costs identified in the first clause, or solely costs identified in the second clause, or a combination of both, then he may recover under the statute.

Yoder & Frey Auctioneers, 774 F.3d at 1074 (citing *Nexans Wires S.A. v. Sark-USA, Inc.*, 166 F. App'x 559, 563 (2d Cir. 2006)).

As such, Plaintiffs' allegation that they expended more than $5,000 investigating Defendants' actions is sufficient to plead the "loss" required to state a viable CFAA violation. *See id*. at 1074 (quoting *A.V. ex rel. Vanderhye v. iParadigms, LLC*, 562 F.3d 630, 646 (4th Cir. 2009)) ("holding that 'loss' is broadly defined and 'plainly contemplates … costs incurred as part of the response to a CFAA violation, including the investigation of an offense.'").

iii. Authorization

Lastly, Defendants argue that Plaintiffs' CFAA claim fails because Defendants were authorized to access Mr. Moore's rmoore@theepicureangroup.com emails as Defendants owned and administered

the account. Defendants also argue that Plaintiffs expressly consented to Defendants' access. Plaintiffs argue that Mr. Moore owned the account as he purchased the Outlook license through which he accessed it. Plaintiffs also argue that even if Defendants owned and administered the account or Plaintiffs gave Defendants some access to it, Defendants exceeded their permitted authorization when they accessed the contents of Mr. Moore's emails.

The Sixth Circuit interprets "without authorization" in the CFAA to mean accessing a computer "without sanction or permission." *Pulte Homes, Inc. v. Laborers' Int'l Union of N.A.*, 648 F.3d 295, 304 (6th Cir. 2011) (quoting *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1132-33 (9th Cir. 2009)). The statute defines "exceeds authorized access" as "access[ing] a computer with authorization and … us[ing] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). "Under this definition, 'an individual who is authorized to use a computer for certain purposes *but goes beyond those limitations* … has 'exceed[ed] authorized access.'" *Pulte Homes*, 648 F.3d at 304 (emphasis in original) (quoting *LVRC Holdings*, 581 F.3d at 1133). "In contrast, 'a person who uses a computer 'without authorization' *has*

no rights, limited or otherwise, to access the computer in question.'" *Id.* (emphasis in original) (quoting *LVRC Holdings*, 581 F.3d at 1113).

At this juncture, the undisputed evidence reflects that the domain name @theepicureangroup.com and the email addresses associated with that account were maintained and paid for by Defendants' IT company, Propel Technologies. (Massey Decl. ¶ 3, ECF No. 11-1 at Pg ID 530.) The present record does not suggest that ownership of the domain name or control of the accounts were transferred as part of the APA. Mr. Moore's ability to access his rmoore@theepicureangroup.com email through the Outlook license he purchased does not alter that fact. Accordingly, Defendants may have had some authorization with respect to the email accounts associated with the domain name, including the account used by Mr. Moore. (*See id*. ¶ 7 (providing that Mr. Massey helped Mr. Moore with the @theepicureangroup.com accounts, "including assisting with termination of employees, new hires, creation of new accounts, and resetting passwords."). Nevertheless, the Court finds a genuine issue of material fact with respect to how far Defendants' authorization extended with respect to Mr. Moore's emails.

In other words, it is not clear from the record that Defendants were authorized to access the contents of the rmoore@theepicureangroup.com account. Defendants may have had the authority to access the emails if they were stored on

Defendants' server. *See, e.g., Sargeant v. Maroil Trading, Inc.*, No. 18-81070, 2018 WL 3031841, at *7 (S.D. Fla. May 30, 2018) ("The common understanding of an entity 'maintaining' a server would include that entity having the technological ability (i.e. the password) and the legal right to access the server."); *Freedom Calls Found. v. Bukstel*, No. 2006 WL 845509, at *27 ("To the extent that prior e-mails sent to Defendant's [work] email account *are stored on Plaintiff's computer system*, Plaintiff has the right to search those stored emails.") (emphasis added). However, the record currently reflects that the emails associated with @theepicureangroup.com were stored on Microsoft's servers. (*See* Compl. ¶¶ 25-27, ECF No. 1 at Pg ID 6-7; Massey Dep. at 19, ECF No. 10-4 at Pg ID 444.) Further, Mr. Moore states in his declaration that he never consented or gave Mr. Massey permission to view, print, or copy his personal emails. (Moore Decl. ¶ 8, ECF No. 10-5 at Pg ID 456); *see also NovelPoster v. Javitch Canfield Grp.*, 140 F. Supp. 3d 938, 945-46 (N.D. Cal. 2014) (concluding that there was a question of fact with respect to the plaintiffs' CFAA claim because although the defendants were granted some access to the business email accounts and were provided the administrative password which enabled them to access individual

email accounts and change passwords, "that does not mean that the defendants were *authorized* to do so").

For these reasons, the Court cannot conclude at this time that Plaintiffs' CFAA claim fails based on the authorization element.

C. Federal Wiretap Act

The Federal Wiretap Act prohibits the interception of electronic communications such as email. 18 U.S.C. § 2511. "Intercept" is defined in the statute as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." *Id.* § 2510(4). In *Luis v. Zang*, 833 F.3d 619 (6th Cir. 2016), the Sixth Circuit held "that the acquisition of a communication must be contemporaneous with its transmission in order for an 'intercept' to occur." *Id*. at 628. In reaching this conclusion, the court joined all the circuit courts that had previously considered the issue. *See id*. (citing cases from the Third, Eleventh, Ninth, and First Circuits). Defendants argue that Plaintiffs' claim fails under the statute because Defendants never intercepted Mr. Moore's email, as that term is defined.

In their Complaint, Plaintiffs allege that Defendants' "interception" of Mr. Moore's emails violated the Federal Wiretap Act, 18 U.S.C. § 2510. Nevertheless, Plaintiffs "must … allege facts that, when accepted as true, give rise to a reasonable inference that [Defendants] contemporaneously acquired the

communications." *Luis*, 833 F.3d at 629 (citing *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)). Unlike the complaint in *Luis*, *id.* at 630-31, Plaintiffs' pleading lacks such facts. The absence of such facts is particularly noteworthy where Plaintiffs had the opportunity to depose Mr. Massey in the State Court Action to determine how he accessed Mr. Moore's emails and specifically what emails he reviewed.[3]

Thus, the Court concludes that Plaintiffs have not adequately alleged a violation of the Wiretap Act.

D. Stored Communications Act

Under the Stored Communications Act ("SCA"), it is a crime to:

> (1) intentionally access[] without authorization a facility through which an electronic communication service is provided; or
>
> (2) intentionally exceed[] an authorization to access that facility;
>
> and thereby obtain[], alter[], or prevent[] authorized access to a wire or electronic communication while it is in electronic storage in such system ….

[3] In his declaration, Mr. Massey states that the program he used to search Mr. Moore's emails does not have the capability to contemporaneously intercept emails. (Massey Decl. ¶¶ 11-12, ECF No. 9-4 at Pg ID 194.) While the Court does not find it necessary to rely on this information to address Plaintiffs' Wiretap Act claim, it finds it significant that Plaintiffs deposed Mr. Massey in the State Court Action, inquired about the program Mr. Massey used to review Mr. Moore's emails, and could have sought information to show that Mr. Massey did in fact contemporaneously intercept emails.

18 U.S.C. § 2701(a). "Facility" is not defined in the statute, but courts have found that the term refers to "'network service providers, which includes telephone companies, internet or e-mail service providers, and bulletin board services.'" *Kornotzki v. Jawad*, No. 19-cv-6689, 2020 WL 2539073, at *3 (S.D.N.Y. May 19, 2020) (quoting *Walker v. Coffey*, 956 F.3d 163, 168 (3d Cir. 2020)). Like the CFAA, the SCA establishes a civil cause of action for "any person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind[.]" *Id*. § 2702(a).

Defendants seek dismissal of Plaintiffs' SCA claim arguing first that, as the provider of the email services, Defendants are exempt from liability under the statute. Defendants next argue that the claim fails because Mr. Moore authorized Defendants' access. Finally, Defendants maintain that they lacked the necessary intent to establish liability.

Defendants' second argument does not entitle them to dismissal of Plaintiffs' SCA claim for the reasons discussed with respect to Plaintiffs' CFAA claim. The Court turns to Defendants' other arguments.

i. Exceptions

As to Defendants' first argument, the SCA exempts from liability "the person or entity providing a wire or electronic communications service." 18 U.S.C. § 2701(c)(1). Citing *Fraser v. Nationwide Mutual Insurance Co.*, 352 F.3d

107, 114 (3d Cir. 2003), and *Joseph v. Carnes*, 108 F. Supp. 3d 613, 616 (N.D. Ill. 2015), Defendants argue that the exemption applies to private employers that provide emails services. In *Fraser*, however, the defendants provided electronic communication services (i.e., they administered and stored the company email on company servers). *Fraser*, 352 F.3d at 115 ("[W]e hold that, because Fraser's e-mail was stored on Nationwide's system (which Nationwide administered), its search of that e-mail falls within § 2701(c)'s exception to Title II."); *see also Walker v. Coffey*, 956 F.3d 163, 169 (3d Cir. 2020) ("Penn State's search of its own server to produce Walker's emails is not prohibited by section 2701 …."). The emails accessed in *Joseph* were archived in a database maintained by the hosting company rather than the third-party service provider. 108 F. Supp. 3d at 615.

Courts have held that the exception in § 2701(c)(1) applies only to entities that provide the services to access the internet, as opposed to entities that purchase services through third parties. *Kornotzki v. Jawad*, No. 19-cv-6689, 2020 WL 2539073, at *3 (S.D.N.Y. May 19, 2020) (quoting *In re Jetblue Airways Corp. Privacy Litig.*, 379 F. Supp. 2d 299, 307-08 (E.D.N.Y. 2005) (holding that "JetBlue does not become an 'electronic communication service' provider simply because it maintains a website that allows for the transmission of electronic communications between itself and its customers")). Relatedly, courts hold that an

employer is authorized to search its employees' emails "only where the employer actually administered and stored the company email system on company servers." *Id*. (citing *Freedom Calls*, 2006 WL 845509, at *27; *Fraser*, 352 F.3d at 115; *Williams v. Rosenblatt Sec. Inc.*, 136 F. Supp. 3d 593, 607 (S.D.N.Y. 2015)); *see also Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548, 560 (S.D.N.Y. 2008) (holding that an employer was not authorized to access a former employee's Hotmail account because "the employee … did not store any of the communications which his former employer now seeks to use against him on the employer's computers, servers, or systems …); *Steinbach v. Village of Forest Park*, No. 06 C 4125, 2009 WL 2605283, at *5 (N.D. Ill. 2009) ("Forest Park purchases Internet access from a third-party provider, and does not itself provide Internet service for the purposes of the exception. The alleged invasion, therefore, is not authorized by statute, as Defendant suggests, and Plaintiff has properly alleged an unauthorized intrusion.").

As discussed above, the email addresses containing the @theepicureangroup.com domain name are Microsoft Office 365 accounts and the emails associated with those accounts are stored on a Microsoft server in the cloud. The exception therefore does not apply.

ii. Intent

The SCA provides a civil cause of action for damages or other relief to any person "aggrieved by any violation of [the SCA] in which the conduct constituting the violation is engaged in with *a knowing or intentional* state of mind[.]" 18 U.S.C. § 2707(a) (emphasis added). It is "the conduct constituting the violation" that must be done knowingly and intentionally. *Long v. Insight Commc'ns of Cent. Ohio, LLC*, 804 F.3d 791, 797 (6th Cir. 2015). Thus, Defendants must have "intentionally accesse[d] without authorization" or "intentionally exceed[ed] an authorization to access" Mr. Moore's emails. 18 U.S.C. § 2701(a). Citing to Mr. Massey's statement in his declaration that he believed he and Mr. Dickerson were authorized to view Mr. Moore's email as the license holder and administrator of the @theepicureangroup.com Office 365 accounts, Defendants maintain that the requisite intent is lacking in this case.[4] (Mot. at 22, ECF No. 9 at Pg ID 58 (citing Massey Decl. ¶ 13, ECF No. 9-4 at Pg ID 194.)

As discussed earlier, however, there is a genuine issue of material fact with respect to the extent of Defendants' authorization in connection with the @theepicureangroup.com email accounts. Plaintiffs should have the opportunity to engage in discovery relevant to the extent of that authorization and what

[4] Contrary to Defendants' assertion (Reply at 5 n.2, ECF No. 11 at Pg ID 524), Plaintiffs did respond to this argument (Resp. at 23 n.4, ECF No. 10 at Pg ID 389.)

individuals other than Mr. Massey understood that authorization to be, particularly as Mr. Massey was acting at someone else's direction when he accessed Mr. Moore's emails. The facts Plaintiffs allege in the Complaint are sufficient to suggest that Defendants acted knowingly and intentionally.

E. Civil Conspiracy

Plaintiffs allege in their Complaint that Defendants conspired to violate the CFAA, Wiretap Act, and SCA. "'A civil conspiracy is an agreement between two or more persons to injure another by unlawful action.'" *Hensley v. Gassman*, 693 F.3d 681, 695 (6th Cir. 2012) (quoting *Hooks v. Hooks*, 771 F.2d 935, 943-44 (6th Cir. 1985)). The plaintiff must show: (a) "'that there was a single plan,'" (2) "'that the alleged conspirator shared in the general conspiratorial objective,'" and (3) "'that an overt act was committed in furtherance of the conspiracy that caused injury to the [plaintiff].'" *Id.* (quoting *Hooks*, 771 F.2d at 944). Defendants first argue that Plaintiffs' conspiracy claim fails under the intra-corporate conspiracy doctrine. Defendants next argue that the claim fails because there is no viable tort to support the claim.

i. Intra-Corporate Conspiracy Doctrine

The intra-corporate conspiracy doctrine provides that "if 'all of the defendants are members of the same collective entity, there are not two separate 'people' to form a conspiracy.'" *Barrow v. City of Hillview, Ky.*, 755 F. App'x

801, 806 (6th Cir. 2019) (quoting *Hull v. Cuyahoga Valley Joint Vocational Sch. Dist. Bd. of Educ.*, 926 F.2d 505, 510 (6th Cir. 1991)). The doctrine draws "on a common sense insight that a person cannot conspire with himself" and "teaches that, since a corporation only acts through its officers, a group of corporate officers acting within the scope of employment cannot create a conspiracy." *Bays v. Canty*, 330 F. App'x 594, 594 (6th Cir. 2009) (internal quotation marks and citation omitted). The Sixth Circuit has recognized that, applied too broadly, "the intracorporate conspiracy doctrine … could immunize all private conspiracies from redress where the actors coincidentally were employees of the same company." *Johnson v. Hills & Dales Gen. Hosp.*, 40 F.3d 837, 840 (6th Cir. 1994). "Aware of this possibility, courts have created a 'scope of employment' exception that recognizes a distinction between collaborative acts done in pursuit of an employer's business and private acts done by persons who happen to work at the same place." *Id*.

Defendants argue that the intracorporate conspiracy doctrine bars Plaintiffs' civil conspiracy claim as Mr. Dickson is the majority owner and an employee of Dickson & Associates. In response, Plaintiffs contend that the doctrine does not apply because Defendants do not admit that Mr. Dickson acted within the scope of his employment when he instructed Mr. Massey to access Mr. Moore's emails.

The facts alleged, however, reflect that Mr. Dickson was acting within the scope of his employment.

Mr. Massey served as the IT Administrator for the entities owned by Mr. Dickson, which included the Epicurean Group. Mr. Dickson instructed Mr. Massey to search Mr. Moore's emails during the State Court Action against Mr. Dickson and the Epicurean Group. Mr. Dickson was sued in that action in connection with the business. Thus, the intra-corporate conspiracy doctrine bars Plaintiffs' civil conspiracy claim against Defendants.

ii. Underlying Tort

Defendants also argue that Plaintiffs' civil conspiracy claim fails as a matter of law because there is no underlying tort alleged. *Marks One Rental, Inc. v. Auto Club Group Ins. Co.*, 55 F. Supp. 3d 977, 988 (E.D. Mich. 2014) (citing *Urbain v. Beierling*, 835 N.W.2d 455, 464 (Mich. Ct. App. 2013) (civil conspiracy requires proof of "underlying tortious conduct")). Plaintiffs fail to respond to this argument. It is, therefore, "deemed conceded and waived." *Boone v. Heyns*, No. 12-14098, 2017 WL 3977524, at *5 (E.D. Mich. Sept. 11, 2017). Moreover, Defendants' argument has merit.

IV. Conclusion

For the reasons stated, the Court concludes that the *Colorado River* doctrine is not applicable to the present matter. The Court further concludes that

Defendants are not entitled to dismissal of Plaintiffs' Computer Fraud and Abuse Act and Stored Communications Act claims (Counts I and III). Plaintiffs, however, fail to adequately plead their Wiretap Act and civil conspiracy claims (Counts II and IV).

Accordingly,

IT IS ORDERED that Defendants' Motion to Dismiss and for Summary Judgment (ECF No. 9) is **GRANTED IN PART AND DENIED IN PART** in that Counts II and IV, only, are dismissed with prejudice.

IT IS SO ORDERED.

s/ Linda V. Parker
LINDA V. PARKER
U.S. DISTRICT JUDGE

Dated: March 22, 2021